Information Technology Security Guidelines

Adopted by the Information Services Board (ISB) on January 31, 2001

Policy No: 402-G1
Supersedes No: N/A
Effective Date: January 31, 2001
Revision Date: June 2003

Also see: 400-P1, 401-S1, Guideline for Reporting and Responding to Computer Crimes Definitions

Table of Contents

Introduction

These guidelines are intended to provide State of Washington agencies with general direction and best practices relating to the implementation of an Information Technology (IT) security program consistent with the State of Washington Information Technology Security Policy and Standards.

Statutory Authority

The provisions of RCW 43.105.041 detail the powers and duties of the ISB, including the authority to develop statewide or interagency information services and technical policies, standards, and procedures.

Scope

These guidelines apply to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage, or use IT services or equipment to support critical state business functions.

Exemptions

The IT Security Policy applies to Institutions of Higher Education, except, pursuant to RCW 43.105.200, when they develop security policies in lieu of the policy statements below that are: a) appropriate to their respective environments, and b) consistent with the intent of the Information Services Board. Such higher education security policies must address:

- Appropriate levels of security and integrity for data exchange and business transactions;
- Effective authentication processes, security architecture(s), and trust fabric(s); and
- Compliance, testing and audit provisions.

Guidelines

I. Business Impact and Risk, Threat, and Vulnerability Analysis Guidelines

Agencies should assess the business impact, risk, threat and vulnerability of mission critical IT investments. The following information provides an overview of the elements of a business impact analysis and a risk, threat, and vulnerability analysis that should be considered:

A. Business Impact Analysis

The initial step of the Business Impact Analysis is to determine the priorities of senior agency management. Next, identify mission-critical business functions, that is, those that are key to the continuation of the organization. If an agency's mission-critical business functions have already been documented, these functions should be reassessed as a regular part of security program maintenance. Suggested criteria for identifying these functions include:

- Maintenance of public health and safety
- Income maintenance for citizens
- Income maintenance for government employees
- Payments to vendors for goods and services
- Requirements for compliance or regulation
- Effect on state government cash flow
- Recovery costs
- Effect on production and delivery of services
- Volume of activity
- Effect on public image
- Inter-system dependency

B. Risk, Threat, And Vulnerability Analysis

Effective IT security programs are primarily a risk management effort. A risk, threat, and vulnerability analysis involves documenting the negative impacts that could result from:

- Accidental or intentional disclosure of data to unauthorized persons
- Unauthorized modification, use, or destruction of data, computer, or telecommunication resources

The purpose of this analysis is to determine the vulnerabilities of IT resources to potential threats and the probability of occurrence of each identified threat. Estimate the potential disruption to each agency program or service area. If a risk, threat, and vulnerability analysis was accomplished in the course of developing a disaster recovery/business resumption plan, include a summary of the conclusions from that analysis. The analysis typically includes the following four steps:

1) Identifying and documenting risks

These risks could result in accidental or intentional disclosure of data to unauthorized persons, unauthorized modifications, and/or use or destruction of data, computer, or telecommunications resources.

There are many natural and human made threats to IT resources (personnel, physical environment, hardware/software systems, telecommunications, applications) and IT operations that could cause a business interruption. The following lists illustrate the range of security threats that should be considered and addressed in the plan if they are pertinent to the agency's circumstances.

Intentional Acts

- Alteration of data
- Alteration of software
- Computer viruses and other malicious code
- Disclosure of confidential information
- Electronic emanations
- Employee sabotage
- External sabotage
- Fraud
- Hackers
- Terrorist activity
- Theft
- Unauthorized use

2) Determining the probability of occurrence of an identified threat

Many physical threats occur regularly. Records of recurring threats, historical occurrences, and statistical probabilities are maintained by organizations such as the Federal Emergency Management Agency (FEMA), the Federal Communications Commission (FCC), and the U.S. Fire Administration. Statistics

on naturally occurring disasters, burglaries, power outages, fires and storms are usually available from local, state, or federal agencies.

An agency should establish a problem tracking system to document physical events that threaten IT resources, such as hardware failures and human attempts to gain unauthorized data access. This information will guide an agency in responding appropriately in a timely manner.

Consider the following factors that affect the probability of a specific threat occurring:

- Geographical location
- Facility environment
- Data sensitivity/importance
- Protection and detection capabilities
- Visibility
- Proficiency level
- Security awareness
- Emergency training
- Staff morale
- Local economic conditions
- Redundancy of control
- Availability and use of written operating and security procedures
- Compliance level (measure of the level of observance or enforcement of security procedures)
- Similar past occurrences

3) Determining the vulnerabilities of IT resources to potential threats

Vulnerability may be measured by the cost an agency would incur if a potential threat actually occurs. For many threats, the vulnerability of the agency can be reduced with appropriate controls. For example, the vulnerability of data retrieval in a distributed database can be partially mitigated through (1) controls that verify that the receiver of each data transmission is the intended receiver and not an intruder, (2) prevention of intruders from intercepting messages, and (3) rigorous management of verification and authorization policies and procedures at distributed database sites and/or sites using the Internet or participating in e-commerce.

Typical vulnerabilities to consider:

- Operating system flaws
- Communications architecture
- Operating procedures

- Access control and authentication
- Security procedures
- The competence of an agency security officer
- Management policies and procedures
- Personnel policies and procedures
- Inadequate audit/security mechanism

4) Estimating the loss potential of an agency program or service area, either by quantitative or qualitative means

Quantitative Approach: The impact of an event is the amount of damage it could cause. The frequency of occurrence of that event is the number of times it could happen. If these two numbers are precisely known, the product of the two would be a statement of potential loss, that is, Loss = (Impact) x (Frequency of Occurrence). Because the exact impact and frequency usually cannot be specified, it is possible only to approximate the loss with an annual loss exposure (ALE). The ALE is the product of estimated impact and estimated frequency of occurrence per year.

Qualitative Approach: The probability and impact of an event are estimated in orders-of-magnitude, i.e.; qualitative terms such as low, medium, or high.

II. Personnel Security Guidelines

The following information provides guidelines for developing, documenting, and implementing the Information Technology Personnel Security aspects of a security program.

A. Hiring practices

Define acceptable levels of prior performance consistent with the sensitivity of the planned work assignment. Consider checks with former peers and/or supervisors at places of prior employment and with references provided.

B. Reference checks

Reference checks that include education, previous employment, and criminal history may be considered for selected personnel who will be required by their job to have access to sensitive information.

C. Security awareness training

Develop a formal security orientation and training program for all employees. The program should be current and comprehensive. It should deal with:

- Applicable laws and/or rules
- Applicable state policies and standards
- Agency security policies, plans, and procedures

- Emerging IT security issues relating to new technologies such as e-government initiatives

D. Employee performance requirements

- Provide specific supervision for new employees working in sensitive areas or on sensitive processes
- Ensure appropriate separation of responsibility and adequate audit trails in sensitive functions

E. Vendor and service personnel monitoring

- Establish procedures for orientation and monitoring of the activities of contractors and service personnel.
- Establish procedures to enact appropriate disciplinary actions or measures for personnel security breaches, including such items as termination of access rights, reassignment, and remedial training.

III. Physical Security Guidelines

The following information provides guidelines for developing, documenting, and implementing Information Technology Physical Security aspects of a security program.

A. Facility characteristics

Where justified, the physical facility should be constructed in accordance with the standards specified in the current edition of National Fire Protection Association (NFPA) publication No. 75, "Protection of Electronic Computing/Data Processing Equipment."

B. Location and layout of the facility

1. Locate large (mainframe) computer equipment in a secure, environmentally controlled facility.
2. If the computer facility is located in a multi-floor facility, assess the risk of damage from plumbing failures, equipment, or occupants of upper floors.
3. Locate the computer facility inconspicuously with no references or direction signs.
4. The general location of the computer room within the overall facility should be outside heavy traffic patterns.
5. Locate mini and/or microcomputer IT resources in an area of authorized traffic.
6. Locate mini and/or microcomputer IT resources in a facility that can be locked during non-prime shift hours, if the critical nature of the resources requires such precaution.
7. Use asset tags or other identification markings for all computer equipment.

8. Compare accounting department fixed asset records of computer equipment and the actual physical equipment on an annual basis.

C. Large computer (mainframe) room physical security attributes

1. Use locking mechanisms to limit computer room access to authorized individuals
2. Ensure that the placement of computer room walls and windows limits access by unauthorized individuals
3. Ensure that the general structure of interior walls are secure and are constructed from the floor to the true, not false, ceiling
4. Use appropriate devices to control access to sensitive data
5. Ensure perimeter security for surrounding areas

D. Physical Access control

1. Identify critical areas and designate specific personnel who require access to these areas.
2. Limit access to the computer operations facility to authorized persons.
3. Arrange for positive identification using pass, key lock, badge system, cipher lock, or other controls for employees, suppliers, and visitors to access the computer room.
4. Change locks or lock combinations to the computer room on a periodic basis.
5. Establish a control system to ensure identification of the individuals having possession of the keys, cards, and badges at any given time.
6. Frequently review the list of assigned key cards or access rights and determine that all persons on the list are still authorized employees.
7. Use logs or special badges for visitors to the computer room.
8. Control access of maintenance and other facilities personnel to the computer room.
9. Require managers to frequently visit the computer room facility on an unannounced basis during a non-prime shift and determine that access control procedures are being followed.
10. Consider establishing a system for the control of packages or containers entering or leaving the restricted area.
11. When an employee is terminated, immediately escort the terminated employee from the computer room and cancel that employee's access rights.
12. Equip any supplementary doors within the computer room facility with exit only locks and audible alarms.
13. Provide for prompt reporting of any actual or suspected hostile act to the appropriate security or law enforcement agency.
14. Use locking devices to secure critical freestanding mini/microcomputer systems.

15. Use locks to secure the chassis of critical mini/microcomputer system from improper removal of boards and from unauthorized operation, whether or not the system is attached to its work platform.
16. Ensure that critical mini/microcomputer workstations are properly locked, that work areas are clear of programs and diskettes, and that locking keys are properly secured during off-shift hours.

E. Data storage and telecommunications controls

1. Establish access, fire, and other controls for the prime data storage facility that is appropriate and consistent with procedures used in the main computer room facility.
2. Establish procedures for logging data in and out of the media library.
3. Establish access, fire, and other controls for the telecommunications control area, which are appropriate and consistent with other computer room procedures.
4. Ensure that cabling of telephone or local network lines from remote devices to the telecommunications facility are shielded or obscured from view.

F. Off-site media storage

1. Ensure that media storage meets needs for archival and/or rotational access.
2. Ensure that storage of paper media, magnetic media, or both, is allowed.
3. Ensure that media storage area meets agency needs for common vaulting, safe-deposit boxes, and/or electronic vaulting.
4. Ensure that storage security needs will be satisfied through use of guards, TV monitors, third-party surveillance, and/or automated security systems.
5. Ensure that storage-building environment provides adequate protection from fire, electrical problems, civil disturbance, and natural disasters.

G. Mobile/remote computing security control

1. Ensure that the use of laptops and mobile computing devices such as personal digital assistants (PDA) are properly controlled. Appropriate encryption solutions should be employed to prevent the compromise of data.
2. Ensure that employees are aware of the risks of stolen or compromised remote computing devices.

IV. Data Security Guidelines

The following information provides guidelines for developing, documenting, and implementing Information Technology Data Security program.

A. Agency data security policy statements

Each agency should publish and distribute a data security policy statement addressing such subjects as:

1. Ownership, custodial, and user information security responsibilities
2. Protection of copyrighted material
3. Automated information access control
4. Appropriate use of secure network sessions

B. Software Version Control and Currency

1. Establish version control policies and procedures for development and maintenance
2. Track and maintain a log of all software changes
3. Use appropriate automated version control toolkits

C. Access control techniques

1. Establish policies and procedures for data access.
2. Define user responsibility for data file access and use.
3. Develop access authorization requirements.
4. Identify sensitive data and specify access rights.
5. Establish procedures for authorization for non-routine access and use.
6. Use other hardware/software access control features as appropriate.
   - Database system features
   - File and data management capabilities of the operating system
   - Data encryption
   - Terminal locks/software locks
   - Security access software systems
7. Ensure that communication lines and controller are adequately protected from damage as well as unauthorized access.
8. Review files that have not been flagged as being password protected and determine whether any should be protected.

D. Data entry processes

1. Establish source data entry authorization procedures as appropriate. Include the following:
   - Authorization signatures
   - Separation of responsibility for data entry and authorization
   - Password and other appropriate security and accounting codes for on-line data entry
   - Operator identification and audit trail

2. Provide for balance and control procedures including:
   - Batch and/or hash totals
   - Check digits
   - Verification

E. Processing accuracy

Establish processing accuracy controls:

- Running file balance totals
- Batch totals
- Processing cycle transaction counts and dollar or hash totals
- Separation of responsibility for operation and control checking
- Sensitive document controls
- Processing audit trails

F. Distribution of output reports and introduction or release of data

Monitor the distribution of output reports as well as the introduction or release of data and program files.

1. If users pick up output reports from the computer operations facility, ensure that only authorized persons may pick up their reports.
2. If an office courier or mail distribution system is used for output report distribution, establish procedures to ensure that reports go only to appropriate recipients and that confidential reports are sealed.
3. Establish procedures for the production and distribution of key documents such as payroll checks.
4. Provide for authorization, logging, and audit trail for non-routine distribution of system output.
5. Provide for disposal of unclaimed output.
6. Establish controls over releasing data files to outside users and ensure that adequate levels of approval are required.
7. Establish procedures for bringing data and program files into the computer system and control the risk of exposure to computer viruses through the introduction of such files.
8. Establish controls covering the import or export of data through any LAN gateways to other computerized systems beyond the LAN, the use of office automation equipment for non-business applications, and the introduction of non-authorized software into the LAN.

G. Data and program back-up

1. Data and program back-up security planning should address:
   - Specification of data and programs that require no back-up

- Specification of data and programs that require a secure on-site back-up
- Specification of data and programs that require both on-site and off-site back-up
- Storage of back-up copies of critical files, documentation, and forms. Store back-up copies of critical files, documentation, and forms in a secure, off-site location

2. Determine what records will be needed to restore service for various levels of system failure and establish procedures for the creation, maintenance, verification, and emergency use of back-up data. Consider the following categories of data:
   - Data files that include magnetic tape master files, disk dumps, and transaction files
   - Application programs
   - Job-control language
   - Systems software, including custom software
   - Program and systems documentation
   - Operational documentation
   - Security, back-up, and recovery procedures
   - Audit records
3. Each data file should be categorized in accordance with the sensitivity and importance of the information it contains. Periodically, select several key applications and ensure that key versions of data files and documentation and special forms are stored in the off-site location. Establish an inventory listing of all items in the off-site location and keep it current.

H. Media Protection

Establish procedures for control and disposition of data storage media containing sensitive data.

- Control and erasure of scratch media
- Control of checkpoint/restart data
- Control of log or journal files
- Control of media library
- Permanent deletion of data or removal of storage media from surplus equipment

I. Controls to prevent unauthorized use or removal of tape files, diskettes, and other media

1. Establish controls over tape files, diskettes, and other media to prevent unauthorized use or removal from IT resource areas.
2. Establish procedures for storing and controlling tape files, diskettes, or other removable media.
3. Specify that labels, volume and serial numbers, and other identifiers consistent with the computer operating system are used for all files.
4. Outline the procedures for implementing retention schedules as outlined by the State Records Committee and the Secretary of State.
5. Establish procedures for the disposal of documents containing personally identifiable information.

J. Guidelines for data encryption management

The purpose of this guideline is to provide agencies a direction and framework for developing an encryption strategy. The standard content represents a minimum set of core information that should be included in each agency's encryption component of their security program.

1. **When to Encrypt**

Agencies should document in their security plan the circumstances under which it is appropriate to encrypt and not encrypt.

At a minimum, encryption should be used when required by federal or state regulations or if there is confidential information with a high risk of unauthorized disclosure. Whether to encrypt, or not, should therefore be a decision made at project inception. **It should be based on a risk assessment of data sensitivity, how the data is accessed, and who is accessing the data, not solely upon whether the data will be accessed through an organization's internal network, the State Government Network, the Inter-Governmental Network, or the Internet.** Finally, the decision to encrypt should be made irrespective of the physical distance between the machines involved in the transfer.

The following evaluation steps are suggested:

a. Perform an assessment on the confidentiality level of data, regardless of use.
b. The confidentiality is based on many factors, such as: operational requirements, regulatory issues, policy and data sensitivity. (See Factors in next section)
c. The confidentiality rating of the data dictates the appropriate level of protection needed.

If the decision is made to encrypt data, there are three areas in which encryption might apply (one, two, or all three might apply):

a. Data at rest (data stored on device),
b. Data in movement (data in transit over a network),
c. Data being viewed or used during an interactive session

2. Factors to Consider for Encryption

State and federal regulations are an important consideration in determining when to encrypt. Some regulations are very specific as to when confidential information must be encrypted. State and Federal regulations governing mental health, alcohol and substance abuse have stringent safeguard requirements that potentially could be enforced through encryption.

Confidential data should be encrypted to protect it from unauthorized disclosure when:

a. It is transmitted over unsecured telecommunications lines
b. It is stored in an electronic file that resides on a computer mainframe, Local Area Network (LAN) client server, or PC hard drive that is readily accessible by individuals who are not authorized to access the information

Confidential information may not require encryption to prevent nondisclosure unless it is transmitted over unsecured telecommunication lines. For example, confidential data stored on a mainframe computer may not require encryption where:

a. The database is not accessible to the general public; and
b. The data are reasonably protected from access by agency employees who do not have a need to know

3. Data Classification Factors

Each agency must define what data is to be regarded as confidential with respect to multiple factors of law, public disclosure, business partners, privacy, and more. Some factors are listed here with examples. These lists are not meant to be exhaustive, but rather helpful in leading the agency to make its own practical decisions regarding secure file transmission. Factors to consider include, but are not limited to:

a. Data that must be encrypted by law.

b. Data that is identifiable as belonging to an individual person or citizen.

c. Data that, if published by a news organization, would be perceived as an invasion of privacy by a citizen.

d. Data that the agency considers "sensitive"

- Citizen's Name
- Citizen's Home, Street or Mailing Address (if not a business)
- Citizen's Telephone Number
- Citizen's Social Security Number
- Citizen's Driver License Number
- Citizen's Personal Identification Number (PIC)
- Citizen's Physical Data (height, weight, eye/hair color, etc.)
- Citizen's Photograph
- Citizen's Medical/Disability Information
- Taxpayer/Financial Information
- Specific Intelligence and Investigative Records
- Sales/Use/Excise Tax Information
- Credit Card and Bank Account Information

e. Specific data contained in sensitive documents (mentioned in privacy statutes) include the following:

- Accident witness and law enforcement reports
- Accident reports
- Coroner report
- Toxicology/Alcohol Reports
- Driving Records
- Case Records of Convictions
- Dealers License Applications
- Driver License
- Identification Cards
- Concealed Pistol Licenses
- Pistol Transfer Records
- Files Maintained for Employees
- Investigative Files
- Complaint Files
- Test Questions
- Medical Certificates

f. Data contained within Financial Statements:

- Tort Claims
- Industrial Insurance Claims
- Membership Lists of Timeshares, Condominiums, Camping Resorts

g. Additional data contained within sensitive documents and records of the agency, including, but not limited to the following:

- Screen Prints
- Copies of Applications
- Microfilm
- Certificates of Ownership, Registration

- Disabled Person Parking Privilege
- Sellers Report of Sale
- Abandoned Vehicle Reports
- Examination Records
- Criminal Histories
- Ineligible to Possess Firearms

4. Choosing your Encryption Products

For satisfying the encryption requirements stated in the Information Technology Security Standards, many products may comply. For example, the secure E-mail requirements might be satisfied by either a secure E-mail package that requires a customer client; or usage of secure messaging - where the E-mail is stored on a secure server and must be "picked up" by the recipient.

Suggested criteria to consider when choosing data products include:

a. Secure File Transfer

Secure exchange of information from one application or user to another. See Information Technology Security Standards for encryption requirements

1) Compatible with all entities (government-to-government, government-to-business, government-to-customer)
2) Conforms to industry-wide standards
3) Supports a wide range of platforms
4) Easily automated with current technologies
5) Supports multiple encryption algorithms and key lengths
6) Audit capability by providing transaction logging

b. Secure E-Mail

Secure delivery of a message from a sender to a receiver. See Information Technology Security Standards for encryption requirements.

1) Compatible with all entities (government-to-government, government-to-business, government-to-customer)
2) Conforms to industry-wide standards
3) Supports a wide range of E-mail clients
4) Integrates with existing E-mail systems
5) Supports multiple encryption algorithms and key lengths
6) Meets agency audit requirements

c. Secure Data Storage

Secure data storage is the protection of data content and changes in data state from its original storage on electronic media by using encryption processes. See Information Technology Security Standards for encryption requirements

1) Compatible with all entities (government-to-government, government-to-business, government-to-customer)
2) Conforms to industry-wide standards
3) Supports a wide range of platforms
4) Easily automated with current technologies
5) Supports multiple encryption algorithms and key lengths
6) Meets agency audit requirements

d. Encryption Methods

Public/Private Key Encryption

The agency encryption plan should incorporate the following concepts if using Public/Private Key Encryption:

1) Certificates used to support encryption of confidential data must be issued by a Washington State licensed Certification Authority (CA) unless required differently by Federal regulatory entities or granting authorities. In no event will encryption certificates be issued unless the issuing CA provides private encryption key backup and recovery services. If an agency must use encryption processes and mechanisms to support its Internet application other than those supported by the Washington State Digital Government framework, it must document the attributes according to the Information Technology Security Standards "Required Risk and Use Assessment Process Step 3 – Selection of Identity Confidence Level Processes and Mechanisms" found in Section I.E.5.
2) User private keys must be protected according to the certificate policy under which they are created. Any potential loss or compromise of a user private key must be reported to the issuing CA immediately. The CA will then revoke the corresponding public key certificate, as per their published Certificate Practice Statement.
3) Key strength will be a minimum of 1024 bits in length.

Secure Sockets Layer (SSL) Protocol

The Secure Sockets Layer protocol is an accepted method for providing a secure channel between Web clients and Web servers by riding on top of the TCP/IP layer of the network protocol stack. SSL provides secure communications, authentication of the server, and data integrity of the message packet. When deemed appropriate by an agency, SSL should be invoked to provide these services for Web-based applications.

Hypertext Transfer Protocol Secure (HTTPS or S-HTTP)
HTTPS is also an accepted method for providing a secure channel between Web clients and Web servers it also provides protection to the TCP/IP layer of the network protocol stack. HTTPS provides secure communications, authentication of the server, and data integrity of the message packet. When deemed appropriate by an agency, HTTPS should be invoked to provide these services for Web-based applications.

S/MIME
S/MIME is a standard for secure electronic mail. It can be used for both authentication (using digital signatures) and privacy (using encryption).

S/MIME melds proven cryptographic constructs with standard E-mail practices. It will also support interoperability between E-mail packages that support the protocol.

If an agency has a need for secure E-mail services, it should document in its security program how S/MIME or some equivalent standard will be used.

e. Technical Guidelines
Encryption should be used for all storage and transmission of sensitive data or as required by law, using the following minimum attributes:

1) Recommendation of 128 bit key encryption or the highest encryption level possible, subject to constraints such as legacy user population, that meets the agency's requirements
2) Securely generated keys
3) Use public key exchange algorithms
4) No e-mail distribution of keys
5) Use of SSL, HTTPS, VPN or other secure connection methods that utilize PKI (digital certificate) technology and Internet based standards for secure network sessions

K. Processing audit trails
Agencies should document how processing audit trails are established for the following:

1. Data entry authorization
2. Operator logging
3. Processing control and balance reports
4. Transaction log files
5. Output distribution logs

L. System access violations

Agencies should document their processes for:

1. Monitoring system access violations for subsequent action and ensure that controls exist to limit such access attempts.
2. Determining if terminal access codes, menu screens, and personal passwords are changed on a periodic basis.
3. Determining that computer system access rights are changed or canceled for individuals who have either terminated employment or changed job responsibilities.
4. Assigning responsibility and procedures for follow-up to unauthorized access attempts.
5. Documenting the procedure for reporting of unauthorized entry or unauthorized attempts to enter or otherwise breach any of the security areas listed above.

M. Virus prevention, detection, and removal

Agencies should establish procedures for virus prevention, detection, and removal that address the following:

1. Appropriate content in the agency security training plan regarding the threat of viruses
2. Use of off-the-shelf scanning tools on servers and desktops with appropriate scanning intervals (no less than once a week)
3. Appropriate response mechanisms to found viruses, including communication to a security administrator and other users who may be at risk
4. Appropriate mechanisms for dealing with detected viruses which cannot be deleted, including disconnection from network and hard disk cleansing
5. Virus scanning of files at the server or firewall level as appropriates
6. Regular reviews of virus scanning logs by system administrators

N. Control of Interactive Internet Technology

Agencies should establish procedures for controlling interactive Internet technologies such as ActiveX and Java scripts that address the following:

1. Appropriate content in the agency security training plan regarding the potential risks of downloading applets
2. Procedures for configuring browsers to accept applets from only trusted servers
3. Procedures for configuring firewalls to block the reception and distribution of applets as required
4. Procedures for regular audits by systems administrators

O. Disposal of Sensitive Hardcopy Data

1. Establish procedures for discarded or outdated sensitive documents that address:
   a. Transportation
   b. Storage
   c. Destruction
2. Dispose of hardcopy documents in accordance with the 1974 federal Privacy Act Guidelines.
3. If the destruction of hardcopies is outsourced, Ensure certificates of destruction are provided.

P. Software Testing

The following guidelines are intended to provide guidance to the security testing of agency designed and implemented software.

1. **Consider the following design vulnerabilities:**
   a. Input overflows, buffer overruns, and no bounds checking
   b. Use of external programs via command interpreters
   c. Unnecessary functionality, such as access to Visual Basic for running programs
   d. Including executable content without a good reason
2. **Consider the following steps in your application development process:**
   a. Do an independent protection audit before release
   b. Use an independent team if necessary
   c. Use good change control in your software update process
   d. Provide a secure manufacturing and distribution mechanism
   e. Provide a Beta-Testing process that helps find flaws
   f. Build a repeatable testing capability
   g. Use constant quality improvement to enhance your security

V. Network and Telecommunications Security Guidelines

The following information provides guidelines for developing, documenting, and implementing the Network and Telecommunications aspects of a security program.

A. Network and telecommunications management

Establish a management function with the authority to establish network and telecommunication standards and procedures for such areas as:

1. Approved equipment types, such as workstations (terminals, microcomputers, mini-computers), which can be introduced to networks
2. Authorization procedures for introducing new equipment to networks
3. Schedules and procedures for authorizing the introduction of communication lines, network addresses, and workstations outside normal operating hours
4. Procedures for the use of any dial-up data lines
5. Determine that there is an appropriate level of management approval for changes to the telecommunications network
6. Communicate the telecommunications network management policies and procedures to users of the network
7. Documenting appropriate use of secure network sessions
8. Documented appropriate use of Virtual Private Networks

B. Inventory control

Document the agency's controls of network and telecommunications equipment inventories and equipment changes. Include all network and data communications equipment on inventory lists, e.g., modems, controllers, workstations, communication lines, and related devices.

1. Ensure that only authorized workstations are connected to the network.
2. Physically verify inventory information by checking the actual workstation installations.
3. Use network diagrams to document both physical and logical connections between telecommunications and other data processing equipment.
4. Verify items of network and telecommunications equipment, wherever located, and trace them to inventory records and to network diagrams to determine that records are accurate.
5. Ensure that network diagrams are stored in a location protected from unauthorized access.
6. Establish procedures for such matters as adding a new workstation or changing a port assignment.
7. Establish a formal testing procedure covering the introduction of any new equipment or changes to the telecommunications network.
8. Provide for verification that formal testing procedures are followed.

C. Secure location of communications equipment

1. If possible, install network and communications equipment in a secure locked room with access limited to authorized individuals.

2. If some communications equipment, such as a communications controller, is kept in the computer operations area, ensure that physical security within that area also is adequate.
3. Authorize only persons with the responsibility and knowledge to use network and/or communications equipment to enter the facility housing that equipment.
4. Locate master workstations that can change the access rights of other workstations or users in secure areas only.

D. Prevention of tampering

1. Place all lines located in areas near the communications equipment room out of sight.
2. Where justified by data sensitivity and potential exposure, label communication lines within the equipment room and elsewhere with a code maintained by telecommunications management rather than with a physical description.
3. In situations where the privacy of data is of great importance, establish procedures requiring the shielding of cables and workstations to prevent electrical emanations, which could be intercepted and read by an unauthorized person.
4. Check the data communications network on a periodic basis for active or passive wiretaps.
5. Ensure data packets transmitted through routers, switches and gateways are appropriately filtered.

E. Terminal, remote job entry (RJE) and network node access security

1. Ensure there are adequate physical access controls
2. Ensure procedures are in place to disable software during "off shift"
3. Create procedures that base hardware/software access restrictions on need of specific device

F. Controls to prevent the introduction of unauthorized programs into computer systems

1. Establish procedures for introducing new software to computer systems.
2. Install virus detection software on computer systems and establish procedures for use of this software.
3. Establish a procedure to list selected directories of computer program libraries and verify that sampled programs are properly authorized.
4. Verify that passwords associated with the security software are changed on a periodic basis.
5. Establish a policy, acknowledged by employees, which prohibits the introduction of unauthorized programs to any computer system.

6. Establish policies to control the general downloading of programs from sources such as computer bulletin boards, Intranets and the Internet.
7. Verify that all connections from the agency network to external networks are approved by and managed by the DIS Security Officer. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures. All connections to approved external networks will pass through DIS-approved firewalls.

G. Network Security Breach Detection

1. Document how the agency supports the following processes:
    a. Operating System and application software logging
    b. Alarm and alert functions
    c. Daily reviews of audit logs from access control mechanisms
    d. Reporting of anomalies
    e. Use of supplemental intrusions detection software on critical servers
    f. Weekly reviews of audit logs on internal protected servers
    g. Use of redundant intrusion detection on highly critical servers
    h. Use of tools to monitor traffic patterns at known concentration points
    i. Integrity assurance process to prevent unauthorized modifications of the firewall configuration.

Typically, checksums, cyclic redundancy checks, or cryptographic hashes are made from the runtime image and saved on protected media. Each time the firewall configuration has been modified by an authorized individual (usually the firewall administrator), it is necessary to update the system integrity online database and save it onto a file system on the network or removable media. If the system integrity check shows that the firewall configuration files have been modified, it will be known that the system has been compromised.

The firewall's system integrity database should be updated each time the firewall is configured or modified. System integrity files should be stored on read-only media or off-line storage. System integrity should be checked on a regular basis on the firewall in order for the administrator to generate a listing of all files that may have been modified, replaced, or deleted.

2. Agencies should include in their security program a description of how they:
    a. Document configuration of the firewall to log all reports on daily, weekly, and monthly bases so that the network activity can be analyzed when needed.
    b. Establish procedures for the periodic examination of firewall logs to determine if attacks have been detected.
    c. Record security-related events on the firewall's audit trail logs.

d. Include as a minimum: hardware and disk media errors, login/logout activity, connect time, use of system administrator privileges, inbound and outbound E-mail traffic, TCP network connect attempts, in-bound and out-bound proxy traffic type.

e. Document configuration of the firewall to:
   - reject any kind of probing or scanning tool that is directed to it so that the firewall does not leak protected information;
   - block all software types that are known to present security threats to a network (such as Active X and Java) to better tighten the security of the network; and
   - Notify the firewall administrator at anytime of any security alarm by E-mail, pager, or other means so that he may immediately respond to such alarm.

H. Network Security Breach Response

Document how the agency plans to support the following processes:

1. Restoration of service after a network break-in
2. Reporting by end-users of anomalies in system performance
3. Review of trouble reports for possible indications of intrusion activity
4. Training on legal issues of incident handling
5. Coordination of potential intrusion activities with the DIS Security Officer
6. Document policies and procedures for restoring the firewall to a working state when a break-in occurs. These should include the following provisions:
   - If it is necessary to bring down the firewall, Internet service should be disabled or a secondary firewall should be made operational - internal systems should not be connected to the Internet without a firewall. After being reconfigured, the firewall must be brought back into an operational and reliable state.
   - In case of a firewall break-in, the agency network/firewall administrator(s) are responsible for reconfiguring the firewall to address any vulnerability that was exploited.
   - The firewall should be restored to the state it was before the break-in (with necessary modifications to prevent re-occurrence of the security violation) so that the network is not left wide open.

I. Use of Virtual Private Networks

Agencies should document how they plan to support the following processes regarding the use of Virtual Private Networks (VPN):

1. Document requirements for a Virtual Private Network and how you plan to review them.
2. Management of security policy equivalency between networks through regular reviews and updates
3. For high impact applications, providing backup connections in the event of an ISP outage or denial or service

4. Integration of a centralized authentication and validation services. The security risk of implementing a VPN solution without a centralized authentication and validation service is identical to consenting to an agency having dual connections to the internet, one being inside the state firewall and the other outside.

VI. Access Security Guidelines

The following information provides guidelines for developing, documenting, and implementing Access Security program.

A. Identification and Authentication

Identification and Authentication (I&A) is the process of recognizing and verifying valid users or processes. The need to determine an authentication mechanism assumes that a decision has been made to allow connectivity to internal systems from the Internet.

There are three major types of authentication available: static, robust, and continuous. Static authentication includes passwords and other techniques that can be compromised through replay attacks. They are often called reusable passwords. Robust authentication involves the use of cryptography or other techniques to create one-time passwords that are used to create sessions. Session hijacking could compromise these. Continuous authentication, primarily achieved through the use of digital certificates, or digital identities, prevents session hijacking.

In order to assist agencies in determining the level of risk associated with their Internet-based application, the following guidelines have been established. Agencies who intend to make information available or conduct transactions with internal users, customers, business partners, or the general public via the Internet should consider and document their risk assessment process based on the following:

Step 1- Determine Mandated Requirements

Before completing an assessment of the appropriate authentication risk level, agencies should first consider the following questions:

- Do any transactions involved in the application in question require a legally binding signature? If the answer is yes, under the Washington Electronic Authentication Act (Chapter 19.34 RCW) a digital certificate issued by a licensed Certificate Authority must be used.
- Is the data or transaction subject to legal or policy-based restrictions outside the scope of the State of Washington Information Technology Security Policy? If the answer is yes, before initiating Step 2 of the assessment process it should be determined if the laws or policies mandate specific authentication mechanisms.
- Does the application involve the processing of high dollar value transactions? If the answer is yes, agencies should consider using a high-level authentication mechanism.

Step 2 - Quantify Potential Impacts

In order to determine the appropriate authentication mechanism, agencies should consider the following questions and issues and quantify their risk assessment of the issues based on the provided guidelines.

B. Authentication Risk Level Determination Chart

Question/Issue	Impact Quantification Guidelines (0-5) **0 - No impact 1 - Minimal impact** **3 - Some impact 5 - High impact**			Total Score by Issue
	Fiscal	Operational	Customer	
What is the potential impact of unauthorized viewing of the data by outside intruders?				
What is the potential impact of unauthorized viewing of the data by legitimate users?				
What is the potential impact of the use of the information assets for other than authorized purposes?				
What is the potential impact of unauthorized deletion, modification, or disclosure of information?				
What is the potential operational impact if the service becomes unavailable (denial of service attacks)?				
What is the potential cost impact if the services provided by the system become unavailable (denial of service attacks)?				
What is the potential public confidence impact if the services or data provided by the system are compromised?				
How important is non-repudiation (inability of a user to deny the initiation of a transaction) to the transactions supported by the system?				
	Overall Score			

Step 3 - Document Conditions and Assumptions

Agencies should prepare a brief narrative which documents the conditions and assumptions used in completing the impact quantification in Step 1.

Step 4 - Determine Level of Risk

After quantifying the impact of potential security and operational issues and documenting conditions and assumptions, agencies should use the table below as a guide for determining the appropriate assurance level. After determining the appropriate risk level, agencies should select an authentication mechanism, which addresses the associated risk.

Impact Score	Level of Risk
0-10	No or little risk
10-20	Low risk
20-30	Moderate risk
30-40	High risk

The table above is intended to provide a guideline for agencies to use in determining the appropriate authentication and protection mechanism based on the level of risk. Other non-security risk factors, such as cost or user impact may cause an agency to select a higher or lower assurance level. In such cases, the agency should document these factors in the narrative completed in Step 3.

For any applications that require authentication, agencies should document in their security plans how they will satisfy the determined level of risk.

C. Digital Signatures and Certificates

If digital certificates are to be used to satisfy a specific level of risk, agencies should document in their security program how this will be done and which type of certificate will be used.

Whether used for purposes of authentication or in support of digital signatures, agencies should subscribe to, and rely upon, digital certificates issued by a Washington licensed certification authority. Pursuant to RCW 19.34.231, if a signature of a unit of state or local government, including its appropriate officers or employees, is required by statute, administrative rule, court rule, or requirement of the Office of Financial Management, a certificate issued by a Washington licensed certification authority for purposes of conducting official public business with electronic records must be used.

D. Logon and Password controls

The following logon and password controls should be considered in agency security programs for site access control:

1. Control all system access through passwords and authorization codes that are validated by security software
2. Require written requests for Logon IDs.
3. Do not allow the use of shared Logon IDs, unless for authorized and approved business justification or if shared Logon IDs are the only practical solutions.

4. Do not allow concurrent use of Logon IDs.
5. Cancel workstation access authorizations when a workstation has been inactive for a specified length of time.
6. Assign Logon IDs to specific individuals rather than functions or groups of individuals.
7. Require passwords be changed as soon as they expire with a limit of one grace logon. Where not supportable by Operating System functionality this should be addressed in policy.
8. Allow owner of Logon ID to change his/her own password.
9. Require the user at his/her first logon to change all passwords. Where not supportable by Operating System functionality this should be addressed in policy.
10. Prevent users from displaying or sharing their passwords.
11. Exclude passwords from batch files.
12. Require passwords not be reused for a minimum of five iterations.
13. Cancel or deactivate Logon IDs when an individual leaves the organization or has a change in responsibilities.
14. Delete or deactivate Logon IDs that have been inactive for more than six months
15. Check personnel records of former employees and determine that their workstation access rights have been deleted.
16. For Internet-based applications that require user authentication, support the use of single authentication and single sign on services

E. Wireless LAN Access

The following items should be considered in agency security programs regarding the use of wireless LANs:

1. Use an industry standard, such as VPN, for authentication and encryption for all wireless traffic to prevent unauthorized access.
2. Use private (non-Internet-routable) IP addresses for wireless devices.
3. Change the wireless access point (AP) name Service Set Identifier (SSID) from the default setting to one that is non-descriptive.
4. Disable beaconing on the device to discourage opportunist hackers.
5. Define in your security program how you will determine no rogue access points exist.

F. Control use of dial-up lines

The following issues should be considered in agency security programs regarding the use of dial-up lines.

1. Control the use of dial-up connections to the computer systems and workstations to prevent unauthorized access attempts.

2. Identify the dial-up connections that are available within the telecommunications network, determine whether the existing dial-up connections are necessary and have been approved by management.
3. Ensure that the security system logs all unsuccessful password or authorization code access attempts.
4. To prevent unauthorized access attempts, in situations where the sensitivity of data is of great importance, install "call back" or "see through" security devices or logical network security passwords on all dial-up connections to the computer system.
5. To prevent accidental line detection, if possible, assign dial-up access numbers to a three-digit exchange number different from the organization's main telephone exchange.
6. Establish procedures for authorizing users to access the dial-up system and screen all users prior to authorizing them.
7. If possible, and where cost-effective, change dial-up access telephone numbers on a periodic basis.

G. Protect voice telecommunication (SCAN) authorization codes for access to long distance dialing

1. Establish procedures to prevent disclosure of SCAN authorization codes.
2. Do not allow employees to share SCAN authorization codes.

H. Recording of telecommunications access

1. Log all telecommunications access to the computer system.
2. Provide for review of computer or telecommunications control logs, and follow-up on exception situations.
3. Ensure that any exceptions have been reviewed and resolved by appropriate levels of management.
4. Develop service level agreements from network service providers to log and support the review of exception situations.

I. Monitoring of manufacturer, software vendor, and third-party access lines to the computer system

1. Monitor the use of manufacturer, software vendor, and third party dial-up access lines to the computer system.
2. Change access numbers and access codes frequently
3. Establish procedure for reporting of unauthorized entry or unauthorized attempts to the appropriate security function

VII. Security Training Guidelines

Agencies should document the aims, training activities, schedule, and administrator activities for agency IT security training. Describe regularly occurring training activities. Employee training should cover the following concepts:

1. Preventing unauthorized access to, damage to, misuse of, or loss of IT hardware, software, data, and facilities
2. Accountability for protection of IT assets
3. Accountability for compliance with software licensing requirements
4. The use or reproduction of copyrighted material
5. An awareness program related to security issues as amplified by the Internet
6. Virus prevention, detection, and removal
7. Interaction Internet Software risks and control
8. Virtual Private Networks

VIII. Law Enforcement Guidelines for Reporting and Responding to Computer Crimes

In the event a computer crime is suspected contact the Washington State Patrol Computer Crimes unit. The Washington Computer Incident Response Center (WACIRC) established guidelines to develop a consistent process to be used by all state agencies when responding to a potential computer crime. To review WACIRC guidelines link to http://www.dis.wa.gov/portfolio/WACIRCGuidelines.pdf

Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to policies, standards, and guidelines. The Department of Information Services is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of the ISB.